Hive Pro

THREAT ADVISORY

US government is being targeted by the Russian SVR aka APT29

TA202106

Threat Level Red

Publish Date – April 18, 2021

Russian SVR is following their predictable trend of exploiting publicly known vulnerabilities against US government to get authenticated access of critical infrastructures. They are targeting COVID-19 research facilities by exploiting VMware Zero-Day vulnerability and deploying WellMess Malware.

The Techniques used by the APT29 includes:

- Exploiting public-facing applications (T11902)
- Leveraging external remote services (T1133)
- Compromising supply chains (T1195)
- Using valid accounts (T1078)
- Exploiting software for credential access (T1212)
- Forging web credentials: SAML tokens (T1606.002)

The 5 vulnerabilities targeted are:

- CVE-2018-13379 Fortinet
- CVE-2019-9670 Zimbra
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-4006 VMware

Actor Details

Name	Known as	Origin	Target Locations	Target sectors
APT 29	Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, Grizzly Steppe, CozyCar, CozyDuke	Russia	Austria, Brazil, China, France, Germany, Hungary, Japan, Mexico, Netherlands, New Zealand, Norway, Portugal, South Korea, Spain, Turkey, Ukraine, United States, Uzbekistan	Academic, Aerospace, Energy, Extractive, Financial Services, Government, Industrials, Engineering, Insurance, Media, NGOs, Nonprofits Oil and Gas, Pharmaceuticals, Technology

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2018-13379	Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	In Fortinet Secure Sockets Layer (SSL) Virtual Private Network (VPN) web portals, an Improper Limitation of a Pathname to a Restricted Directory("Path Traversal") allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.	CWE-22
CVE-2019-9670	Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10	cpe:2.3:a:synacor:zimbra_collaboration_suite:8.7.11:-:*:*:*:*:*:*	In Synacor Zimbra Collaboration Suite, the mailboxd component has an XML External Entity injection (XXE) vulnerability.	CWE-611

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2019-11510	Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4	cpe:2.3:a:pulsesecure:pulse_connect_secure:8.2:-:*:*:*:*:*:* cpe:2.3:a:pulsesecure:pulse_connect_secure:8.3:-:*:*:*:*:*:* cpe:2.3:a:pulsesecure:pulse_connect_secure:9.0:-:*:*:*:*:*:*	In Pulse Secure VPNs, an unauthenticated remote attacker can send a specially crafted Uniform Resource Identifier (URI) to perform an arbitrary file read.	CWE-22
CVE-2019-19781	Citrix ADC and Gateway versions before 13.0.47.24, 12.1.55.18, 12.0.63.13, 11.1.63.15 and 10.5.70.12 and SD-WAN WANOP 4000-WO, 4100-WO, 5000-WO, and 5100-WO versions before 10.2.6b and 11.0.3b	cpe:2.3:o:citrix:application_delivery_controller_firmware:10.5:*:*:*:*:*:*:* cpe:2.3:o:citrix:application_delivery_controller_firmware:11.1:*:*:*:*:*:*:* cpe:2.3:o:citrix:application_delivery_controller_firmware:12.0:*:*:*:*:*:*:* cpe:2.3:o:citrix:application_delivery_controller_firmware:13.0:*:*:*:*:*:*:* cpe:2.3:o:citrix:netscaler_gateway_firmware:10.5:*:*:*:*:*:*:* cpe:2.3:o:citrix:netscaler_gateway_firmware:11.1:*:*:*:*:*:*:* cpe:2.3:o:citrix:netscaler_gateway_firmware:12.0:*:*:*:*:*:*:* cpe:2.3:o:citrix:gateway_firmware:13.0:*:*:*:*:*:*:*	Citrix® Application Delivery Controller (ADC) and Gateway allow directory traversal.	CWE-22
CVE-2020-4006	VMware One Access 20.01 and 20.10 on Linux, VMware Identity Manager 3.3.1 - 3.3.3 on Linux, VMware Identity Manager Connector 3.3.1 - 3.3.3 and 19.03, VMware Cloud Foundation 4.0 - 4.1, and VMware Vrealize Suite Lifecycle Manager 8.x	cpe:2.3:a:vmware:identity_manager:3.3.1:*:*:*:*:*:*:* cpe:2.3:a:vmware:identity_manager_connector:3.3.1:*:*:*:*:*:*:* cpe:2.3:a:vmware:one_access:20.01:*:*:*:*:*:*:* cpe:2.3:a:vmware:one_access:20.10:*:*:*:*:*:*:* cpe:2.3:a:vmware:identity_manager_connector:3.3.1:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:4.0:*:*:*:*:*:*:* cpe:2.3:a:vmware:vrealize_suite_lifecycle_manager:*:*:*:*:*:*:*:*	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector have a command injection vulnerability.	CWE-77

Patch Links

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37033
https://www.securityfocus.com/bid/108693
https://sec.hpi.de/vulndb/details/CVE-2019-9670
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101
https://support.citrix.com/article/CTX267027
https://www.vmware.com/security/advisories/VMSA-2020-0027.html

References

https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF
https://securityaffairs.co/wordpress/116891/cyber-warfare-2/russia-svr-actively-targets-5-flaws.html
https://nvd.nist.gov/vuln/detail/CVE-2018-13379
https://nvd.nist.gov/vuln/detail/CVE-2019-9670
https://nvd.nist.gov/vuln/detail/CVE-2019-11510
https://nvd.nist.gov/vuln/detail/CVE-2019-19781
https://nvd.nist.gov/vuln/detail/CVE-2020-4006